Cassandra Crossing/ Lo stato delle PET

(62)—Le tecnologie per la protezione della privacy non godono di prospettive entusiasmanti e la comunità è a tirar fuori qualche…

Cassandra Crossing/ Lo stato delle PET

(62)—Le tecnologie per la protezione della privacy non godono di prospettive entusiasmanti e la comunità è a tirar fuori qualche spicciolo. Ecco cosa è successo e cosa è lecito attendersi.

15 dicembre 2006—PET sta per *Privacy Enhancing Technologies*—tecnologie per il miglioramento della privacy. Approfittiamo della fine dell'anno per tirare le somme di quanto è stato fatto (o non è stato fatto) nello creazione di nuove applicazioni PET e nello sviluppo delle più importanti tra quelle esistenti.

Una considerazione generale, che riguarda l'intero settore, è non ci sono novità significative; non sono stati annunciati nuovi sviluppi teorici od applicazioni innovative. Sul fronte dell'esistente la situazione è migliore, anche se non completamente soddisfacente.

Qui sotto le PET più significative, cominciando con un evergreen: **Freenet**.

È un'applicazione per la pubblicazione ed il recupero anonimo di informazioni realizzata in linguaggio Java, disponibile su praticamente tutti i sistemi operativi ed in sviluppo dal lontano 1999. A differenza di altre applicazioni simili, che memorizzano i dati in chiaro sui dischi dei pc partecipanti alla rete, Freenet estende la protezione dei contenuti tramite la crittografazione e la suddivisione delle informazioni in un "datastore" crittografato, distribuito e ridondante, che

protegge gli utenti anche da un punto di vista legale.

Freenet è una rete molto utilizzata e popolata di contenuti di vario tipo.
Per la seconda volta nella sua storia sta attraversando una fase piuttosto traumatica di completa riscrittura, che ha causato la nascita di due reti completamente separate tra loro e la conseguente perdita sia di contenuti che di utenti.

Le modifiche principali riguardano l'algoritmo di routing ed il protocollo di trasporto, che passa da TCP ad UDP. Quest'ultima decisione è dovuta alla necessità di poter utilizzare PC posti in reti private (con NAT—Network Address Translation) usando a questo scopo alcune delle tecniche "evasive" impiegate, ad esempio, da Skype. È prevista anche la possibilità di creare gruppi chiusi di utenti interni a Freenet con ammissione ad invito, le cosiddette "Darknet".

Tor (The Onion Routing) è l'applicazione più nuova ed attualmente di maggior impatto per la privacy in Rete.
Consiste in una rete di proxy TCP anonimizzanti che applicano tecniche di crittografazione ripetuta, da cui il nome di Onion Routing—"routing a cipolla", cioè a più strati. È realizzata in linguaggio C, disponibile per i sistemi operativi più diffusi; analogamente a Freenet è implementata non come applicazione ma come protocollo di rete.

A differenza di Freenet non permette di memorizzare informazioni, ma in compenso utilizza un protocollo applicativo (SOCKS) che ne permette l'utilizzo con la maggioranza dei programmi e dei browser esistenti, senza nessuna modifica. Può essere impiegata con qualunque applicazione che utilizzi solo TCP, ad esempio web, chat, posta, ssh, telnet e così via.
È di installazione ed utilizzo estremamente semplici, e possiede estensioni grafiche di controllo (Vidalia) che ne evidenziano il funzionamento in maniera eccezionalmente chiara.

Nella sua storia ha beneficiato di finanziamenti sia dagli ambienti militari che della Electronic Frontier Foundation, ed i suoi core developer, provenienti prevalentemente dal progetto FreeHaven, sono tra i massimi esperti accademici di teoria delle comunicazioni anonime, hanno sviluppato anche in ambiente universitario e gestito professionalmente le attività di sviluppo, producendo un codice di qualità molto alta, decisamente superiore a quello medio sia di applicazioni libere che proprietarie.

Nell'ultimo anno purtroppo lo sviluppo si è molto rallentato per l'esaurimento dei finanziamenti di EFF, ed il gruppo di sviluppo, per attenuare l'azzeramento delle risorse, sta portando avanti collaborazioni con l'ambiente universitario canadese.

Il sito di riferimento, contrariamente alla maggior parte delle applicazioni libere, contiene una documentazione molto completa, sia a livello utente che sviluppatore, in buona parte disponibile anche in italiano.

L'efficacia pratica e l'importanza della rete Tor è confermata anche dalle "at-

tenzioni" che ha ricevuto di recente, in Germania ed in misura minore in Italia, da quegli ambienti che considerano non desiderabile l'esercizio del diritto alla privacy in Rete.

Mixmaster, cioè la nonna delle PET, è una rete di server di posta specializzati che consentono di spedire messaggi in maniera anonima, utilizzando come trasporto la normale posta elettronica SMTP. Con opportune estensioni (nymserver) consente anche di rispondere a messaggi anonimi. È una rete molto utilizzata ma non più sviluppata perchè di gestione ed utilizzo complessi. Si è trovata e si trova anche oggi in prima linea a sostenere gli attacchi di chi vuole azzerare la privacy in Rete; per questo motivo il numero dei remailer Mixmaster si va purtroppo lentamente riducendo.

Mixminion dovrebbe essere la PET che sostituirà Mixmaster risolvendone (si spera) la maggior parte dei problemi.
È una rete di server specializzati che permettono di scambiare messaggi di posta in forma anonima senza utilizzare la normale posta elettronica SMTP, ma comunicando tramite un protocollo specializzato molto più veloce ed affidabile. Automatizza la gestione delle chiavi crittografiche, rendendola anche molto più robusta contro alcuni attacchi di memorizzazione del traffico. Si interfaccia direttamente sia con la posta elettronica normale che con la rete Mixmaster.

Pur essendo già pienamente utilizzabile, Mixminion si trova in una fase di sviluppo estremamente rallentato; questo è dovuto principalmente al fatto che il gruppo dei core developer è lo stesso di Tor. Si puo' dire che in un certo senso Mixminion è attualmente una "vittima" certamente non voluta del successo di Tor. È comunque un software estremamente ben sviluppato, sia nella parte concettuale che in quella realizzativa. È sperabile che benefici presto di alcune ricadute dal progetto Tor, con cui condivide il problema di gestione dei directory server.

Concludendo, la situazione di alcune PET sta arrivando alla maturità, ed almeno due di queste applicazioni sono utilizzabili ed utilizzate da molti utenti, non necessariamente esperti ma anche solo volonterosi.

Lo sviluppo delle nuove PET, Freenet, Mixminion e Tor, si trova però in sofferenza per la mancanza di risorse, sia a livello di sviluppatori volontari che soprattutto di soldi, che consentono di mantenere un livello di sviluppo decente fornendo semplicemente la pagnotta ai core developer attuali, e lasciandoli liberi di concentrarsi sulle PET piuttosto che su altri lavori di semplice sussistenza.

Perciò il solito invito.

È di nuovo Natale; ancora un volta, se ci tenete alla vostra privacy, frugatevi in tasca e donate qualche spicciolo al vostro progetto preferito. Qui per Tor e Mixminion e qui per Freenet.

Scrivere a Cassandra—Twitter—Mastodon

Videorubrica “Quattro chiacchiere con Cassandra”
Lo Slog (Static Blog) di Cassandra
L’archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on December 7, 2023.

Canonical link

Exported from Medium on January 2, 2024.